



**Espacenet**

## Bibliographic data: JP3034084 (A) — 1991-02-14

### RECORDING DEVICE FOR PORTABLE STORAGE MEDIUM

**Inventor(s):** KAWADA MIKI ±  
**Applicant(s):** TOSHIBA CORP ±

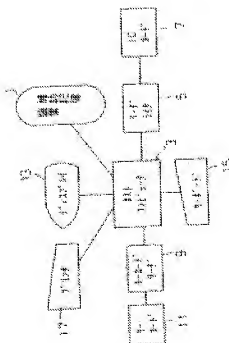
**Classification:** - **international:** *B42D15/10; G06F17/40; G06K17/00; G07F7/08;* (IPC1-7): B42D15/10; G06F15/74; G06K17/00; G07F7/08  
 - **European:**

**Application number:** JP19890166982 19890630

**Priority number(s):** JP19890166982 19890630

### Abstract of JP3034084 (A)

**PURPOSE:** To improve the security of issued data by storing decoding data to be used for the decoding processing of the issued data in a portable electronic device, and reading this decoding data, and decoding the issued data by this decoding data to store it in a portable storage medium. **CONSTITUTION:** The code key, the personal identification number, etc., of the decoding data for decoding the encoded issued data stored as information in an auxiliary storage device 1 are stored previously in a key card 11 consisting of an IC card to constitute the portable electronic device. This decoding data is read out, and the issued data is decoded by this decoding data, and is stored in the IC card 7 as the portable storage medium. Thus, the safety of the decoding data is raised, and the security of the issued data is improved.



Last updated: 14.03.2012   Worldwide Database   5.7.38; 92p

⑫ 公開特許公報(A) 平3-34084

⑬ Int. Cl.<sup>3</sup>

識別記号

庁内整理番号

⑭ 公開 平成3年(1991)2月14日

G 06 K 17/00  
B 42 D 15/10  
G 06 F 15/74  
G 06 K 17/00  
G 07 F 7/08

S 6711-5B  
5 2 1 6548-2C  
3 3 0 G 7530-5B  
B 6711-5B

8208-3E G 07 F 7/08

G

審査請求 未請求 請求項の数 2 (全5頁)

⑮ 発明の名称 携帯可能記憶媒体への記録装置

⑯ 特 願 平1-166982

⑰ 出 願 平1(1989)6月30日

⑱ 発 明 者 河 田 美 樹 神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 代 理 人 弁理士 三好 秀和 外1名

明 細 書

3. 発明の詳細な説明

[ 発明の目的 ]

(産業上の利用分野)

本発明は、ICカードのような携帯可能記憶媒体に例えば発行者に関する情報またはカード所持者毎の情報等の発行データを記憶する携帯可能記憶媒体への記録装置に関する。

(従来の技術)

ICカードのような携帯可能記憶媒体は、例えば発行データファイル内に格納されている上述のような発行者に関する情報またはカード所持者毎の情報等の発行データが発行システムにより書き込まれて発行される。この発行データが秘密性を要するものである場合には、その発行データは暗号化されて発行データファイル内に格納されており、発行時に復号化されてICカードに書き込まれる。

このように暗号化されている発行データを復号化するために使用される復号化用データ、すなわち暗号キーは、従来、データファイルの形で発行

1. 発明の名称

携帯可能記憶媒体への記録装置

2. 特許請求の範囲

(1) 暗号化された発行データを記憶した記憶手段と、前記暗号化された発行データの復号化処理に使用される復号化用データを格納した携帯可能電子装置と、該携帯可能電子装置に格納された復号化用データを読み出し、この読み出した復号化用データによって前記発行データを復号化する復号化手段と、該復号化手段で復号化された発行データを記憶する携帯可能記憶媒体とを有する携帯可能記憶媒体への記録装置。

(2) 前記携帯可能電子装置は暗証番号を記憶した暗証番号記憶手段を有し、前記復号化手段は前記暗証番号記憶手段に記憶された暗証番号を照会した後、前記復号化用データを読み出すことができる読み出し手段を有することを特徴とする請求項

(1)記載の携帯可能記憶媒体への記録装置。

システム内に記憶されていたり、または発行処理を制御するプログラムの中に予め記憶されている。

(発明が解決しようとする課題)

従来、暗号化された発行データの復号化処理に使用される復号化用データ、すなわち暗号キーは、データファイルの形で発行システム内に記憶されていたり、または発行処理を制御するプログラムの中に予め記憶されているため、読み出されたり、変更され易く、安全性に問題がある。

本発明は、上記に鑑みてなされたもので、その目的とするところは、暗号化された発行データの復号化処理に使用される復号化用データの安全性を高め、これにより発行データの安全性を高めた携帯可能記憶媒体への記録装置を提供することにある。

[発明の構成]

(課題を解決するための手段)

上記目的を達成するため、本発明の携帯可能記憶媒体への記録装置は、暗号化された発行データを記憶した記憶手段と、前記暗号化された発行

データの復号化処理に使用される復号化用データを格納した携帯可能電子装置と、該携帯可能電子装置に格納された復号化用データを読み出し、この読み出した復号化用データによって前記発行データを復号化する復号化手段と、該復号化手段で復号化された発行データを記憶する携帯可能記憶媒体とを有する要旨とする。

(作用)

本発明の携帯可能記憶媒体への記録装置では、発行データの復号化処理に使用する復号化データを携帯可能電子装置に記憶し、この復号化データを読み出し、この復号化データによって発行データを復号化して携帯可能記憶媒体に記憶している。

(実施例)

以下、図面を用いて本発明の実施例を説明する。

第1図は本発明の一実施例に係わる携帯可能記憶媒体への記録装置の全体構成を示すブロック図である。同図に示す携帯可能記憶媒体への記録装置は、一例として携帯可能記憶媒体としてIC

カードを使用し、このICカードに例えば発行者に関する情報またはカード所有者毎の情報等の発行データを記憶して発行する発行システムを構成するものであり、該発行データを暗号化して発行データファイルとして記憶している補助記憶装置1および全体の動作を制御するホストコンピュータ3を有する。補助記憶装置1は前記発行データ以外に本発行システムを制御する制御プログラムを記憶している。また、ホストコンピュータ3は制御および一時的にデータを格納するメモリを有する。

ホストコンピュータ3には、リーダー/ライダ5、キーカードリーダー9、ディスプレイ13、キーボード15およびプリンタ17が接続されている。リーダー/ライダ5はホストコンピュータ3の制御のもとに所要の発行データをICカード7に書き込んだり、またはICカード7から情報を読み出す動作を行い、キーカードリーダー9は携帯可能電子装置を構成するICカードからなるキーカード11から情報を読み出したたり、または情報、具体

的にはオペレータがキーボード15から入力した暗証番号をキーカード11に供給する装置であり、キーカード11には情報として補助記憶装置1に記憶されている暗号化された発行データを復号化するための復号化データである暗号キーおよび暗証番号等が記憶されている。

また、ディスプレイ13は本発行システムの操作手順や状態をオペレータに表示し、キーボード15は発行システムを操作して作動させるための各種指令および情報を入力するために使用される。更に、プリンタ17は日時、発行データファイル名、カード番号および発行枚数等を印字出力し、これによりICカード7の発行記録を作成している。

第2図は前述した補助記憶装置1に記憶されている発行データファイルのフォーマットを示している。同図に示す発行データファイルは、6バイトのカード番号21を先頭として複数の発行データ23、すなわち同図において一例としてData 1, Data 2, . . . のように名付けられた

発行データ23が並んで記憶されている。

次に、第3図を参照してカード発行処理の作用を説明する。

まず、ディスプレイ13に表示される指示に従って暗証番号および暗号キーが記憶されているキーカード11をキーカードリーダー9に挿入する(ステップ110)。それから、本発行システムのエベレータがキーボード15から暗証番号を入力すると、この入力された暗証番号はキーカードリーダー9を介してキーカード11に供給され、キーカード11においてキーカード11に既に記憶されている暗証番号との照合が行われる(ステップ120)。この照合が成立すると(ステップ130)、この時点でキーカード11に記憶されている復号化用データである暗号キーの読み出しができる状態になる。なお、この暗号キーは後述するステップ170において読み出され、ステップ210において補助記憶装置1からの暗号化された発行データを復号化するために使用される。照合が成立しない場合には、キーカード11はキー

カードリーダー9から排出され、カード発行処理は中止される(ステップ130)。

暗証番号の照合が成立した場合には、オペレータはディスプレイ13に表示される指示に従って更に発行するデータファイル名、開始カード番号、発行枚数および発行者暗証番号をキーボード15から入力する(ステップ140)。そして、これらの入力情報はホストコンピュータ3のメモリに記憶される。ホストコンピュータ3は、入力された発行データファイルが補助記憶装置1内に記憶されているか否かチェックする(ステップ150)。また、記憶されている場合には、更にこの発行データファイルをホストコンピュータ3のメモリから読み出し、入力された開始カード番号から発行枚数分のカード番号までが該発行データファイル内に記憶されているか否かチェックする(ステップ160)。記憶されていることが確認されると、補助記憶装置1はキーカードリーダー9を介してキーカード11に記憶されている復号化データである暗号キーを読み出し、ホストコンピュータ

3のメモリに記憶する(ステップ170)。

それから、オペレータはディスプレイ13に表示される指示に従ってICカード7をリーダー/ライター5に挿入し(ステップ180)、このICカード7のメモリに予め記憶されている発行者暗証番号を前記ステップ140でキーボード15から入力した発行者暗証番号と照合し、オペレータが発行者であることを確認する(ステップ190)。照合が成立すると(ステップ200)、ホストコンピュータ3はステップ140で入力されたホストコンピュータ3のメモリに記憶されている開始カード番号、例えば第2図に示すように「000001」の開始カード番号に属する発行データ23の「Data n」、更に具体的には第1番目の発行データ23の「Data 1」を前記ステップ170で読み出した暗号キーおよび発行システムの制御プログラムに組み込まれた復号化ルーチンによって復号化処理し(ステップ210)、この復号化された「Data 1」をICカード7にリーダー/ライター5を介して書き込む(ステップ22

0)。

ICカード7に「Data 1」を書き込んだ後は、該カードに対する全データの書き込みが終了したか否かをチェックし、終了していない場合には、発行データを更新して終了するまで前記ステップ210、220の復号化処理およびICカード7への書き込み処理を行う(ステップ230、240)。例えば、一人分の発行データの個数をmとすると、「Data 1」に続いて「Data m」までの各発行データに対して復号化処理およびICカード7への書き込みを行う。

開始カード番号に属する全データの書き込みが終了すると、ICカード7はリーダー/ライター5から排出される(ステップ250)。それから、ステップ140で指定されたICカード7のすべてに対してデータ書き込み処理が終了したか否かチェックされ(ステップ260)、すべて終了していない場合には、カード番号をインクリメントしてステップ180に戻る(ステップ270)。そして、このようにインクリメントされた次のカー

ド番号、例えば「00002」のカード番号のICカード7の挿入がディスプレイ13の表示により要求され、このICカード7が挿入されると、このICカード7に対するステップ190～230の処理が同様に繰り返される。

ステップ140で入力された発行枚数分の書き込みが終了すると（ステップ260）、キーカードリーダー9からキーカード11が挿出され（ステップ280）、それからプリンタ17から発行記録表として、発行年月日、発行データファイル名、発行されたデータのカード番号および発行枚数等が印字出力され、処理は終了する（ステップ290）。

なお、前記ステップ130、150、160、200のチェック処理において、チェック不良となり、エラーが発生した場合には、ディスプレイ13にエラーメッセージが表示され、処理が終了または中断される。

〔発明の効果〕

以上説明したように、本発明によれば、発行デ

ータの復号化処理に使用する復号化データを携帯可能電子装置に記憶し、この復号化データを読み出し、この復号化データによって発行データを復号化して携帯可能記憶媒体に記憶しているので、携帯可能電子装置からの復号化データの読み出し時に、例えば暗証番号の照合を行ったり、または復号化データを記憶した携帯可能電子装置を発行データから分離して、例えば金庫等に保管することにより、復号化データの安全性を高め、これにより発行データの安全性を一段と向上することができる。

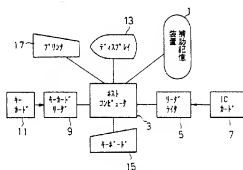
#### 4. 図面の簡単な説明

第1図は本発明の一実施例に係る携帯可能記憶媒体への記録装置の構成を示すブロック図、第2図は第1図の記録装置に使用される発行データファイルのフォーマットを示す図、第3図は第1図の記録装置の作用を示すフローチャートである。

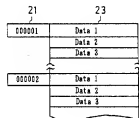
- 1…補助記憶装置、
- 3…ホストコンピュータ、
- 5…リーダー/ライター、

- 7…ICカード、
- 9…キーカードリーダー、
- 11…キーカード。

代理人弁護士 三好秀和



第1図



第2図

